SC MEDIA

- SC US
- SC UK

Show Search Bar

Search SC Media Search

- News
  - Features
  - Executive Insight
  - The SC Blog
  - Business & Finance
  - Cyber-security events calendar
- Cyber-crime
  - Ransomware
  - Data breaches
  - APTs/Cyber-espionage
  - Malware
  - Phishing
  - Insider threats
- Network Security
  - Mobile security
  - Cloud security
  - Privacy & Compliance
  - Vulnerabilities
  - IoT
  - Email security
- Products
  - Group Tests
  - SC Buyer's Guide 2017
- Video
- Events
  - SC Congress London
  - Editorial Roundtable Series
  - SC Awards Europe
- Expert reports
- Webcasts

- Log in
- ●
- Register

The Cyber-Security source
by Doug Olenick

February 16, 2018

Cryptocurrency mining crimeblotter, Apache CouchDB & other vulnerabilities

The amount of illegal cryptocurrency mining that is now taking place makes keeping track a difficult task, but here is a quick roundup of what was has been spotted over the last few days.

The amount of illegal cryptocurrency mining that is now taking place makes keeping track a difficult task, but here is a quick roundup of what was has been spotted over the last few days.

- Cisco Talos has detailed a six-month long investigation into a specific mining campaign that used phishing scams, tied to Google Ad words to lure victims that stole tens of millions of dollars.
- Meanwhile, Trend Micro has found and explored miners exploiting two vulnerabilities found in Apache CouchDB to install cryptominers on systems.
- A third method making news is the Trickbot trojan being used to create a man in the middle attack to steal credentials from people as they purchase bitcoin.

Talos' research found the criminal grop, dubbed CoinHoarder, buying Google Ad Words linked to search terms associated with cryptocurrency, such as blockchain or Bitcoin wallet. The ads then appear near the top of a search page as an advertisement for a Bitcoin wallet site. However, the link provided in the ad takes victims to a professional looking, but malicious, landing page, such as blockchain.info. Once on the landing page the victim is served phishing information in the person's native language, as based on the IP address that would enable the thieves to remove bitcoin from their wallets.

“The reach of these poisoned ads can be seen when analysing DNS query data. In February 2017, Cisco observed spikes in DNS queries for the fake cryptocurrency websites where upwards of

200,000 queries per hour can be seen during the time window the ad was displayed," Talos wrote.

Most of the victims were from non-English speaking nations, with particular attention paid to those in Africa and other developing countries where banking is difficult and local currencies unstable making Bitcoin a 'safe' haven.

This method is so efficient that Talos believes Coinhoarder has stolen more than US$ 50 million (£36 million) over the last three years. The group greatly benefited from Bitcoin's recent skyrocketing valuation. To keep the scam running all that is done is purchase more Ad Words.

While Trend Micro did not have a monetary amount stolen by those using the Apache CouchDB vulnerabilities, the number of detected attacks has spiked during the last three weeks.

The flaws at issue are Apache CouchDB JSON Remote Privilege Escalation Vulnerability (CVE-2017-12635) and Apache CouchDB _config Command Execution (CVE-2017-12636). Both of which were patched in November 2017.

Trend found that CVE-2017-12635 is first exploited to configure a CouchDB account with admin abilities which is then used to authenticate the remote code execution flaw in CVE-2017-12636. Once inside a system the malware injected detects and disables competing miners and then downloads and executes Coinhive.

CouchDB is a somewhat popular data base management system and is used by some large corporations giving those looking to take advantage of unpatched systems access to some pretty powerful resources, Trend noted.

"However, in our view, the system being targeted is not as important as the existence of vulnerabilities that can be exploited," the report said, "As long as there's a chance to exploit an RCE (remote code execution), the threat actors will take advantage of it."

Using a remote code execution flaw to run a cryptominer is even more attractive because it is a low-risk operation, but also high reward because the price of the various digital currencies are climbing.

The TrickBot trojan began its life attacking banking and financial interests, but IBM's X-Force Team has found the group behind it has expanded into the cryptocurrency stealing business. This particular case has TrickBot being used to place itself in the middle of a cryptocurrency transaction and steal from those purchasing Bitcoin and Bitcoin cash using a credit card.

"This particular attack targets both the bitcoin exchange website and that of the payment service to grab the coins and route them to an attacker-controlled wallet," X-Force said.

TrickBot is a great tool here, IBM said, as it is uses webinjections to implant itself in both the bitcoin wallet and payment card websites where it can grab the information needed to steal the currency. Unlike the Ad Words scam, TrickBot requires a relatively high level expertise from the criminal.

"Having researched the attack tactics TrickBot applied to this cryptocurrency coin theft, we can see that, while it relies on existing mechanisms, the scheme required extensive research of the targeted sites, their web logic and the security controls they use," IBM said.

- f
- 🐦
- in
- G+

- 👽
- 💬
- 🖨

Topics:

- Apache
- Cisco
- Cryptocurrency
- Mining
- Vulnerabilities

0 Comments **SC Media UK** **Login**

♡ **Recommend** **Share** **Sort by Newest**

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

ALSO ON **SC MEDIA UK**

Severe security flaw found in Windows 10-bundled password manager

1 comment • 3 months ago

Kay Donovan — When I first read about it, the articles were pretty misleading, they almost presented it like it was a flaw of the native

Linux systems can still be hacked via USB sticks

1 comment • 25 days ago

Waqas — Please, for the sake of whatever you love most in your life put the link to the original research so readers can check for further

FIDO promotes device-based unified authentication standards

1 comment • 4 months ago

Sillie Abbe — FIDO is said to have recommended that biometrics be used together with a password. Have someone heard whether FIDO requires or

Russia bans non-compliant VPNs - a blow to privacy and free speech?

1 comment • 4 months ago

LeopoldT — if they do register, does that mean they're essentially a tool by government to track your data? for now, at least those not operating

✉ **Subscribe** **Add Disqus to your siteAdd DisqusAdd** 🔒 **Privacy**

Related Articles

App zero-day flaw exploited to fool users into malicious downloads

BY Bradley Barth Feb 14, 2018

Drive-by cryptomining targeting millions of Android devices

BY Robert Abel Feb 14, 2018

Lazarus Group back from the dead - again - with renewed phishing campaign

BY Jay Jay Feb 14, 2018

Crypto exchange BitGrail and token developer Nano in coin theft dispute

BY Bradley Barth Feb 13, 2018

Most read on SC

- Google gets sued for denying "right to be forgotten" request
- Hackers using blockchain to keep authorities at bay & to sustain operations

- Chrome 65 update ready, contains 45 security fixes
- Government calls for revamp in IoT security; will manufacturers listen?
- Hospitality industry is key infosec battleground

SC Media UK arms cyber-security professionals with the in-depth, unbiased business and technical information they need to tackle the countless security challenges they face and establish risk management and compliance postures that underpin overall business strategies.

USER CENTRE

About Us

Contact Us

Advertise

Partner's Corner

RESOURCES

Issue Archive

OTHER

Privacy Policy

Terms & Conditions

MORE SC SITES

Follow SC Media UK